WHAT IS CLAIMED IS:

1. A method for generating pseudo-random numbers, comprising the steps of:

loading a current seed value S_j from a non-volatile storage;

loading a value, E, representative of environmental randomness;

loading a value, C, representative of configuration data;

generating a new seed value, S_{j+1}, in accordance with the following equation:

$$S_{j+1} = f(S_j; A; C; E),$$

wherein f represents a selected encryption algorithm , and B is a second constant, and wherein S_j is concatenated with A, which is concatenated with C which is concatenated with E;

writing the new seed value S_{j+1} to the non-volatile storage;

generating a key, K, in accordance with the following equation:

$$K = f(S_j; B; C; E),$$

wherein B is a second constant; and

generating a pseudo-random number output, P_n, in accordance with the following equation:

$$P_n = f_{3DES}(K, P_{n-1}),$$

where f_{3DES} represents the operation of triple DES encryption hardware, and P_{n-1} is the previously generated pseudo-random number.

2. The method of claim 1, wherein the function f comprises the FIPS 180 secure hash standard algorithm (SHA).

3. The method of claim 1, wherein the value E includes at least 80 bits of entropy.

4. The method of claim 1, wherein the seed S_j is 160 bits in length.

5. The method of claim 1, wherein the seed S_j is 256 bits in length.

6. The method of claim 1, wherein the seed S_j is 512 bits in length.

7. The method of claim 1, wherein an initial value of P_0 is 0.

8. The method of claim 1, further comprising the steps of loading values for the first and second constants A and B from a protected ROM address.

9. The method of claim 8, wherein the first and second constants A and B further incorporate a copyright notice embedded therein.

10. The method of claim 1, wherein the f_{3DES} hardware is operated in output feedback mode.

11. The method of claim 1, wherein the f_{3DES} hardware is operated in dual counter mode.

12. A computer-readable medium incorporating one or more instructions for generating pseudo-random numbers, the instructions comprising:

one or more instructions for loading a current seed value S_j from a non-volatile storage;

one or more instructions for loading a value, E, representative of environmental randomness;

one or more instructions for loading a value, C, representative of configuration data;

one or more instructions for generating a new seed value, S_{j+1}, in accordance with the following equation:

$$S_{j+1} = f\ (S_j;\ A;\ C;\ E),$$

wherein f represents a selected encryption algorithm , and B is a second constant, and wherein S_j is concatenated with A, which is concatenated with C which is concatenated with E;

one or more instructions for writing the new seed value S_{j+1} to the non-volatile storage;

one or more instructions for generating a key, K, in accordance with the following equation:

$$K = f\ (S_j;\ B;\ C;\ E),$$

wherein B is a second constant; and

one or more instructions for generating a pseudo-random number output, P_n, in accordance with the following equation:

$$P_n = f_{3DES}(K,\ P_{n-1}),$$

wherein f_{3DES} represents the operation of triple DES encryption hardware, and P_{n-1} is the previously generated pseudo-random number.

13. The computer-readable medium of claim 12, wherein the function f comprises the FIPS 180 secure hash standard algorithm (SHA).

14. The computer-readable medium of claim 12, wherein the value E includes at least 80 bits of entropy.

15. The computer-readable medium of claim 12, wherein the seed S_j is 160 bits in length.

16. The computer-readable medium of claim 12, wherein the seed S_j is 256 bits in length.

17. The computer-readable medium of claim 12, wherein the seed S_j is 512 bits in length.

18. The computer-readable medium of claim 12, wherein an initial value of P_0 is 0.

19. The computer-readable medium of claim 12, further comprising one or more instructions for loading values for the first and second constants A and B from a protected ROM address.

20. The computer-readable medium of claim 19, wherein the first and second constants A and B further incorporate a copyright notice embedded therein.

21. The computer-readable medium of claim 12, wherein the f_{3DES} hardware is operated in output feedback mode.

22. The computer-readable medium of claim 12, wherein the f_{3DES} hardware is operated in dual counter mode.